REALPATH

The destination string buffer must be long enough to hold the return file path. Never use this function (or do so at very high potential risk).

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-02

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 5305 bytes

Attack Category	• Path spoofing or confusion problem
Vulnerability Category	• Buffer Overflow • Unconditional
Software Context	• File Path Management
Location	• stdlib.h
Description	realpath expands all symbolic links and resolves references to '/./', '/../' and extra '/' characters in the null terminated string named by path and stores the canonicalized absolute pathname in the buffer of size PATH_MAX named by resolved_path. The resulting path will have no symbolic link, '/./' or '/../' components. Never use this function (or do so at very high potential risk) It is broken by design since it is impossible to determine a suitable size for the output buffer. According to POSIX a buffer of size PATH_MAX suffices, but PATH_MAX need not be a defined constant, and may have to be obtained using pathconf(). And asking pathconf() does not really help, since on the one hand POSIX warns that the result of pathconf() may be huge and unsuitable for mallocing memory. And on the other hand pathconf() may return -1 to signify that PATH_MAX is not bounded. The libc4 and libc5 implementation contains a buffer overflow (fixed in libc-5.4.13). Thus, suid programs like mount need a private version.
APIs	<table><tr><th>Function Name</th><th>Comments</th></tr><tr><td>realpath</td><td></td></tr></table>
Method of Attack	An attacker could cause input of a densely symbolic path that expands to a very long length and could cause an overflow of the destination buffer.
Exception Criteria	

[1] http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

Solutions

Solution Applicability	Solution Description	Solution Efficacy
All occurrences of realpath().	Use realpath() if one or more of the following conditions apply: 1. Risk of overflow is small or inconsequential if failure occurs. (Application is such that a default path can be set if failure occurs, but this does not prevent the overflow). 2. Maximum possible path has been prototyped and is within PATH_MAX limits (if PATH_MAX is defined)	Highly variable.

Signature Details

char *realpath(const char *path, char *resolved_path);

Examples of Incorrect Code

```
int main(int argc, char *argv[]) {
...
char *symlinkpath = argv[1];
char actualpath
[strlen(symlinkpath)];
char *ptr;
ptr = realpath(symlinkpath,
actualpath);
...
}
```

Examples of Corrected Code

```
int main(int argc, char *argv[]) {
...
char *symlinkpath = argv[1];
char actualpath [PATH_MAX];
char *ptr;
ptr = realpath(symlinkpath,
actualpath);
...
```

<table>
<tr><td></td><td>}</td></tr>
<tr><td><b>Source References</b></td><td>• Viega, John & McGraw, Gary. <i>Building Secure Software: How to Avoid Security Problems the Right Way</i>. Boston, MA: Addison-Wesley Professional, 2001, ISBN: 020172152X, pg. 147
• http://maconlinux.net/linux-man-pages/en/realpath.3.html
• The IEEE and The Open Group. realpath - resolve a pathname[3]. <i>The Open Group Base Specifications Issue 6</i>; IEEE Std 1003.1, 2004 Edition (2004).</td></tr>
<tr><td><b>Recommended Resource</b></td><td></td></tr>
<tr><td><b>Discriminant Set</b></td><td><table>
<tr><td><b>Operating Systems</b></td><td>• Windows
• UNIX (All)</td></tr>
<tr><td><b>Languages</b></td><td>• C
• C++</td></tr>
</table></td></tr>
</table>

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[1] mailto:copyright@cigital.com